

# Almond



Édition 2024/2025

## Observatoire des cybermenaces

L'Europe connaît une accélération des  
attaques depuis 18 mois

TLP:CLEAR



# SOMMAIRE

Sommaire

L'équipe projet

Préface

**01** ■ Ransomwares : l'invasion continue

**02** ■ Le business lucratif des Infostealers

**03** ■ Fuites de données : une année productive pour les attaquants

**04** ■ L'observatoire CWATCH

**05** ■ DDoS : l'Europe dans le collimateur

**06** ■ Vulnérabilités : le poids sur les stratégies défensives

Références



# L'ÉQUIPE PROJET

Almond tient à remercier l'ensemble des experts qui ont permis la réalisation de ce Threat Landscape.



**Chloé**  
**GRÉDOIRE**

Cyber Threat Intelligence  
Analyst



**Manon**  
**GUEGUEN**

Cyber Threat Intelligence  
Analyst



**Mathias**  
**GARCIAU**

Manager  
SOC / CERT / CTI CWATCH



**Mélodie**  
**CELIN**

Chargée de Communication &  
Marketing Senior

Aucune IA n'a été maltraitée  
lors de la rédaction de ce Threat  
Landscape 2025, entièrement  
rédigé par des humains !

# EDITO

## Le nouveau visage de la cybermenace : défis et impératifs

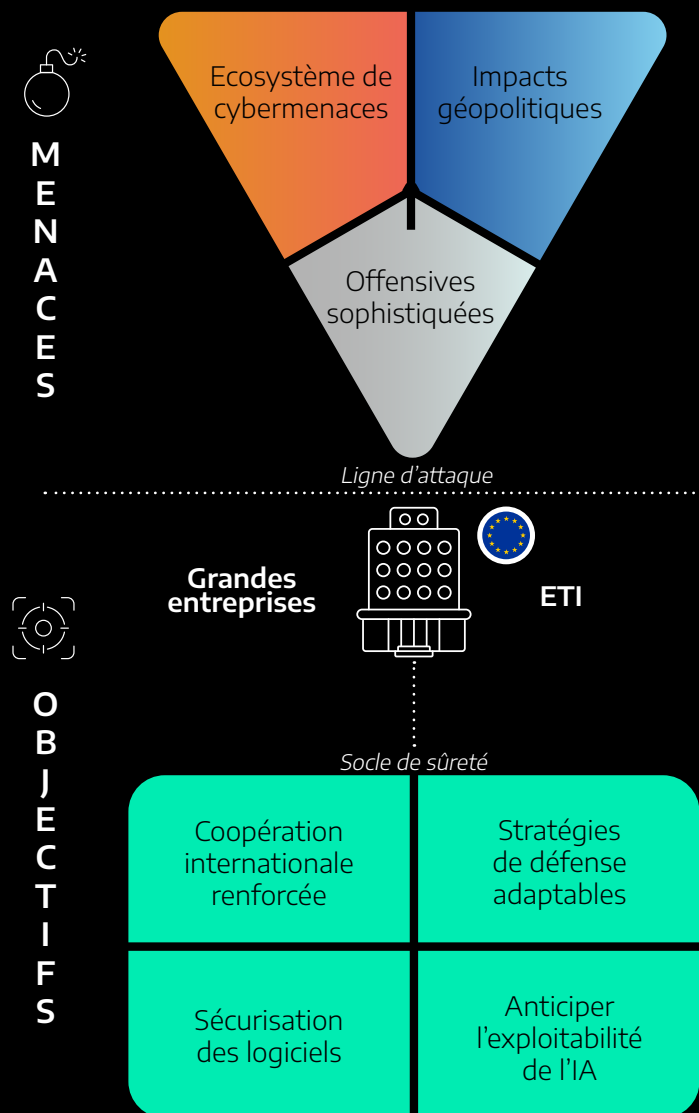
À mesure que le paysage des menaces cybernétiques évolue, il le fait à un rythme vertigineux, façonné par un contexte géopolitique sans précédent et des avancées technologiques de pointe. Ces éléments transforment radicalement la nature des attaques, exigeant une vigilance et une adaptation constantes.

Au cœur des tensions géopolitiques actuelles, l'Europe se retrouve en première ligne, cible privilégiée des cybercriminels qui affinent leurs méthodes à une vitesse alarmante. Nous assistons à l'émergence de tactiques inédites, incluant des attaques DDoS hyper-volumétriques et l'exploitation sophistiquée de l'intelligence artificielle, qui redéfinissent le champ de bataille numérique.

Ces nouvelles approches mettent particulièrement à l'épreuve les grandes entreprises et les ETI. La complexité de leurs systèmes d'information, combinée à une certaine inertie organisationnelle, les rend particulièrement vulnérables à des attaques de plus en plus raffinées. Face à cette menace croissante, les Jeux Olympiques de Paris 2024 illustrent une vraie prise de conscience et d'une préparation accrue, faisant de cet événement un cas d'étude en matière de coopération sécuritaire.

Dans ce contexte difficile, il devient impératif d'établir une coopération renforcée, tant au niveau européen qu'international, pour combattre efficacement ces menaces. Par ailleurs, la responsabilité des éditeurs de logiciels dans la sécurisation des environnements numériques doit être clairement affirmée et intégrée dans les stratégies de défense cybernétique.

L'heure est à la mobilisation : ensemble, renforçons nos défenses et anticipons les défis de demain pour sécuriser notre avenir numérique.



01.

## RANSOMWARES : L'INVASION CONTINUE

Le nombre de victimes dans le monde a **augmenté** de près de 29% entre 2023 et 2024.

En France, on constate une évolution de près de 82% (vs 2023, 155 victimes répertoriées).

En 2024, la valeur médiane de détection d'une menace (MTTD) observée par le CERT Almond était de deux jours.

Ces chiffres nous rappellent que les **attaquants ont toujours un temps d'avance sur la défense.**

### LES OBSERVATIONS CWATCH

5 642

victimes de  
ransomwares  
en 2024 dans  
le monde

2 170

victimes de  
ransomwares  
en 2024 en  
Europe

282

victimes de  
ransomwares  
en 2024 en  
France

Mean Time to Detect  
(MTTD)



Break-out-time



Mean Time to Respond  
(MTTR)

01.

## RANSOMWARES : L'INVASION CONTINUE

### Ce qui se cache derrière les classements

Les données peuvent être incomplètes, elles ont été essentiellement constituées à partir de sources occidentales.

Ce rapport est construit à partir des victimes rendues publiques sur les wall of shame des groupes cybercriminels. Attention, ils n'affichent pas la totalité de leurs victimes **comme nous avons pu le constater au sein de notre équipe de réponse à incident, seule une attaque sur 2 est revendiquée.**

## VICTIMOLOGIE DES RANSOMWARES

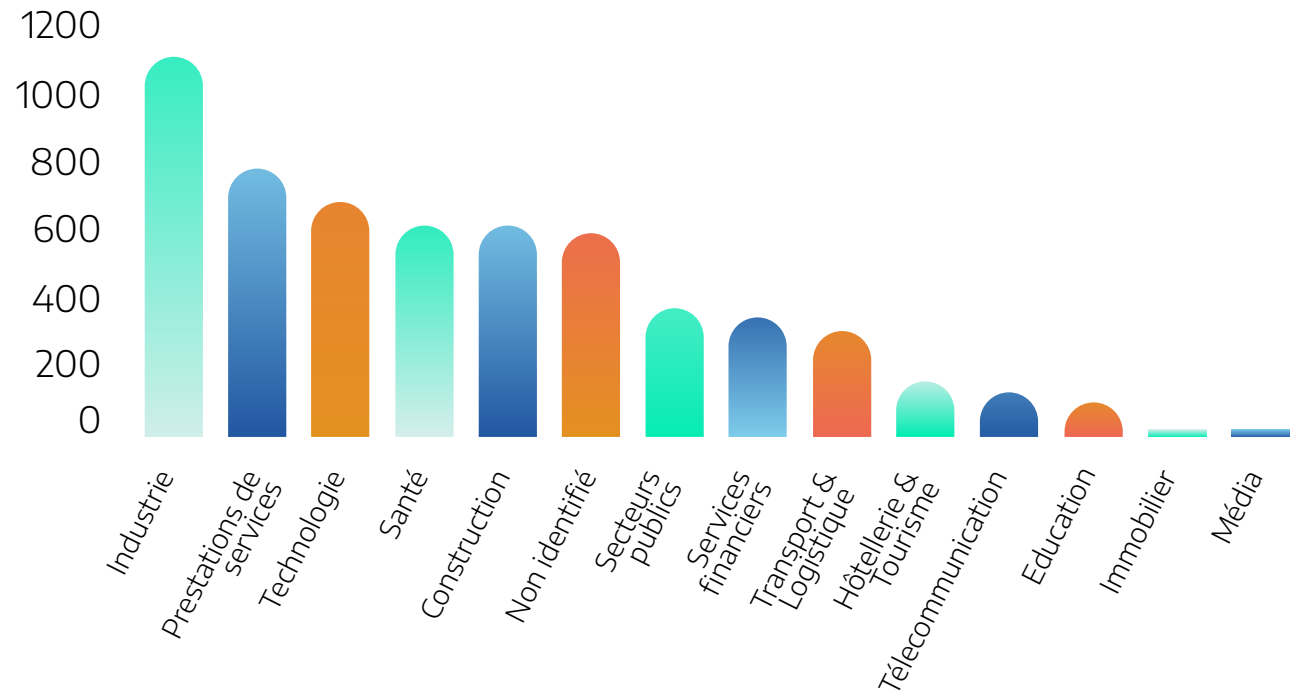
Le terme **industrie** englobe une majeure partie des infrastructures critiques telle que l'énergie, l'aérospatiale, la production agricole, les infrastructures hydrauliques, etc. C'est un secteur, comme celui de la **santé** qui attire les attaquants, car particulièrement **médiatisé**. C'est aussi un **moyen de gagner en notoriété** pour les groupes émergents et d'affirmer leur présence dans l'écosystème concurrentiel des RaaS.

TOP 3

01. Industrie

02. Prestations de services

03. Technologie



01.

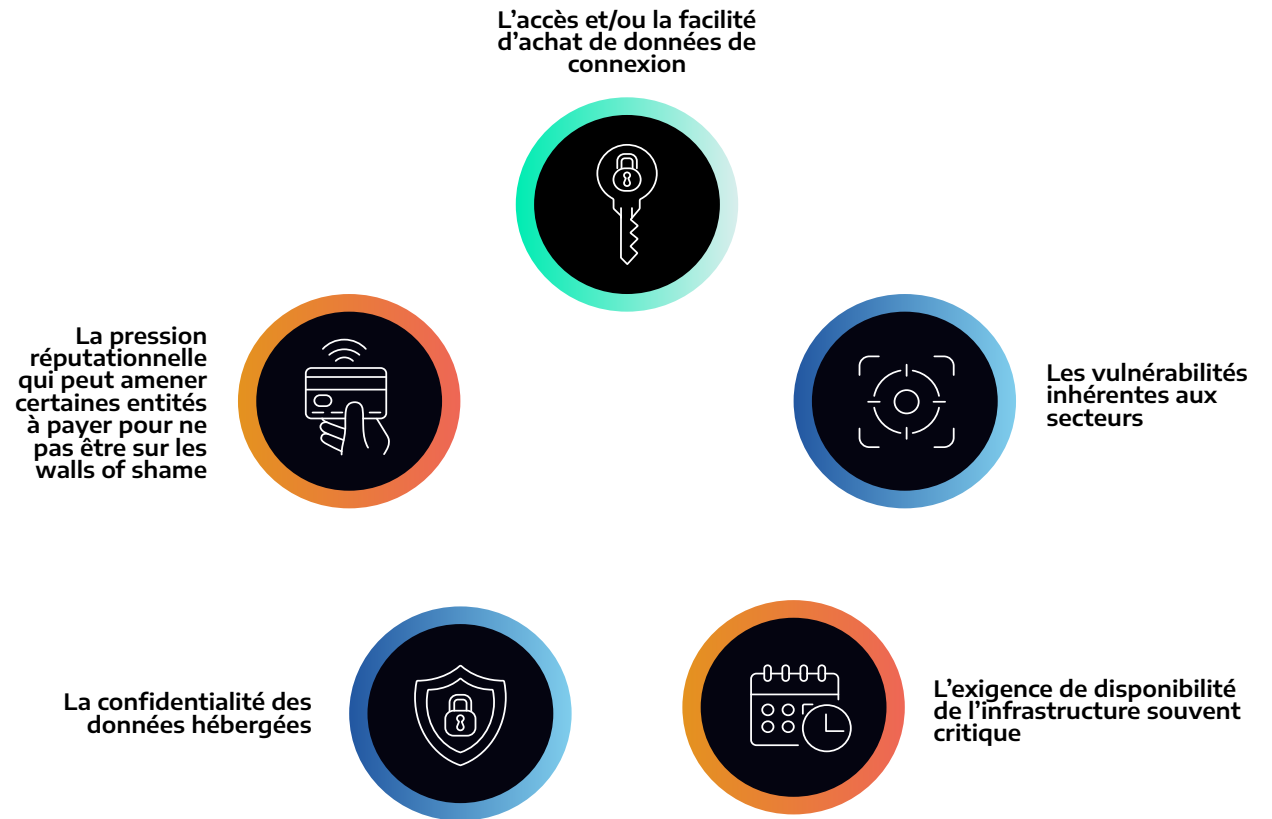
## RANSOMWARES : L'INVASION CONTINUE

Almond observe sur cette édition que les secteurs de l'**industrie** et des **prestations de services** conservent respectivement les première et deuxième places.  
Voir le [Threat Landscape Almond 2023/2024](#)



### VICTIMES POTENTIELLES PAR LES GROUPES DE RANSOMWARE

Le top 10 des secteurs les plus touchés par des attaques de rançongiciel reste sensiblement le même depuis plusieurs années. Afin de **maximiser leur succès** en termes de gain financier, les groupes opérant des rançongiciels ciblent régulièrement les entités **en mesure de payer**. Les critères de sélection peuvent être :





01.

## RANSOMWARES : L'INVASION CONTINUE

### Place à la nouvelle génération

On observe une recomposition du paysage de la menace des ransomwares avec la montée en puissance de plusieurs groupes et la permanence assurée par **LockBit** qui reste néanmoins en suspens.

Il est commun au sein de l'écosystème des ransomwares que des groupes se forment pour faire un maximum de victimes pendant une période donnée avant de se dissoudre pour continuer leurs activités sous une nouvelle identité.

### COMPARAISON DE LA RÉPARTITION 2023/2024

#### TOP 2024

Lockbit	518
RansomHub	505
Play	337
Akira	282
Hunters	215
Medusa	206
BlackBasta	174
Qilin	171
Bianlian	161
Incransom	155

#### TOP 2023

Lockbit	1030
AlphV	416
ClOp	384
Play	301
8Base	269
Bianlian	178
BlackBasta	176
Malas	173
Akira	160
Medusa	145

Selon nos données, **LockBit** reste en tête en dépit des opérations de déstabilisation menées par les autorités coordonnées de plusieurs pays dès février 2024 et l'arrestation en décembre de plusieurs membres du groupe, [dont un développeur Rostislav Panev](#).

Il est suivi de près par **RansomHub** qui se serait développé à partir du code du ransomware [Knight](#), élément qui a constitué la base de son essor.

Quant à **Play**, ce groupe aurait potentiellement bénéficié d'une collaboration ou sinon d'un intérêt émanant du groupe coréen [Jumpy Pisces](#) pour mener certaines opérations.

En 2023, le groupe **LockBit** était suivi de **AlphV** et **ClOp** qui ont tous les deux connu un net ralentissement de leurs activités cette année. **Les revendications de AlphV ont chuté de 87% et celles de ClOp de 96%**. Par ailleurs, **le groupe 8Base a connu une baisse de 47% de ses activités. Les activités de Play ont augmenté de 12%**.



01.

## RANSOMWARES : L'INVASION CONTINUE

### Des impacts à multiples facettes

La réputation, un actif immatériel sous haute menace... Après avoir lancé son attaque contre le club de football de Bologne, **RansomHub** a diffusé des données concernant **des informations financières, personnelles et médicales des joueurs ainsi que des contrats de parrainage**. On y trouvait aussi des **plans stratégiques** concernant les transferts et **les jeunes talents, les données des supporters, des employés et des structures du club**.

## TIMELINE DE LA REPRISE DES ACTIVITÉS À COPPELL

### Peur sur la ville

En novembre 2024, **RansomHub** a ciblé la ville de Coppell, au Texas, et le Minneapolis Park and Recreation Board. L'attaque a perturbé le WIFI, les activités du tribunal municipal, les services de la bibliothèque et les plateformes de permis et d'inspection.

### Priorité aux gains

C'est cette année que la demande de rançon la plus conséquente a été observée avec le groupe **Dark Angels** qui a réclamé **75 millions de dollars à Cencora**, une entreprise pharmaceutique américaine. Le **prix moyen** d'une rançon était de 2 millions de dollars en 2023.

La visibilité dont bénéficient les ransomwares en raison de leur impact saisissant pour les victimes ne doit pas dissimuler un **écosystème financier plus complexe** qui profite bien plus à d'autres acteurs malveillants.

**23 octobre**

Cyberattaque détectée et impactant une majeure partie des services de la ville

**1<sup>er</sup> novembre**

Rétablissement des services téléphoniques

**14 novembre**

Rétablissement des formulaires de facturation des services publics

**15 novembre**

Remise en service des bibliothèques locales

**20 novembre**

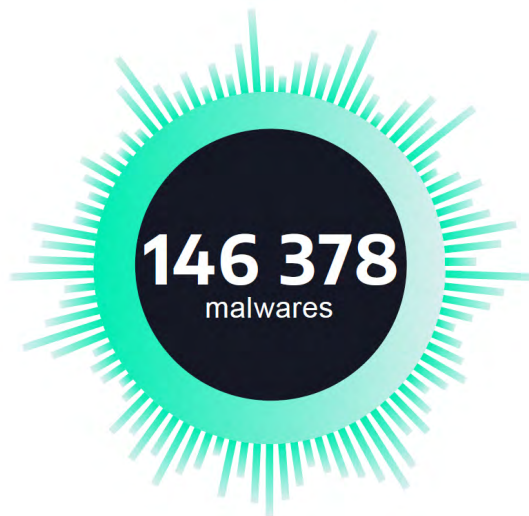
Annulation d'événements municipaux

02.

## LE BUSINESS LUCRATIF DES INFOSTEALERS

Un infostealer est un programme malveillant qui a pour objectif de collecter les données sensibles de type données d'authentification, données bancaires stockées, etc. Comme le Ransomware-as-a-Service, ces programmes sont développés par des groupes puis mis en vente en tant que Malware-as-a-Service au « tout venant ». Le gain financier de la vente des informations collectées a permis, comme pour le business du ransomware, de professionnaliser l'écosystème.

### INFOSTEALERS EN VOGUE



En 2024, près de 146 378 malwares ont été répertoriés par Anyrun, dont une **majorité** avec des fonctionnalités d'infostealers. Cette année confirme la croissance de leurs activités dans le paysage des malwares. Outils peu chers, accessibles facilement et à la portée de « novices », les infostealers sont de plus en plus populaires car le marché de la donnée volée est de plus en plus lucratif. Trop souvent sans même que la victime soit au courant qu'il y a eu exfiltration.



#### Au secours, fuite de données...

Snowflake s'est retrouvé cette année dans la tourmente. Une **campagne à grande échelle** visait à obtenir les données hébergées de clients dans un but lucratif. Ce n'est pas l'entreprise Snowflake qui a été compromise. Il a été mis en évidence dans le cadre de la **réponse à incident** que les accès des clients à leur plateforme Snowflake avaient été récupérés et mis en vente par de **multiples infostealers** tels que **LUMMA, Redline, Vidar et MetaStealer** depuis au moins quatre ans. À cela s'est ajoutée l'absence d'authentification multifacteur sur ces environnements. **L'achat par un threat actor de ces comptes valides a donc permis la compromission d'au moins 100 clients, dont Santander Bank et Live Nation.**

02

## LE BUSINESS LUCRATIF DES INFOSTEALERS

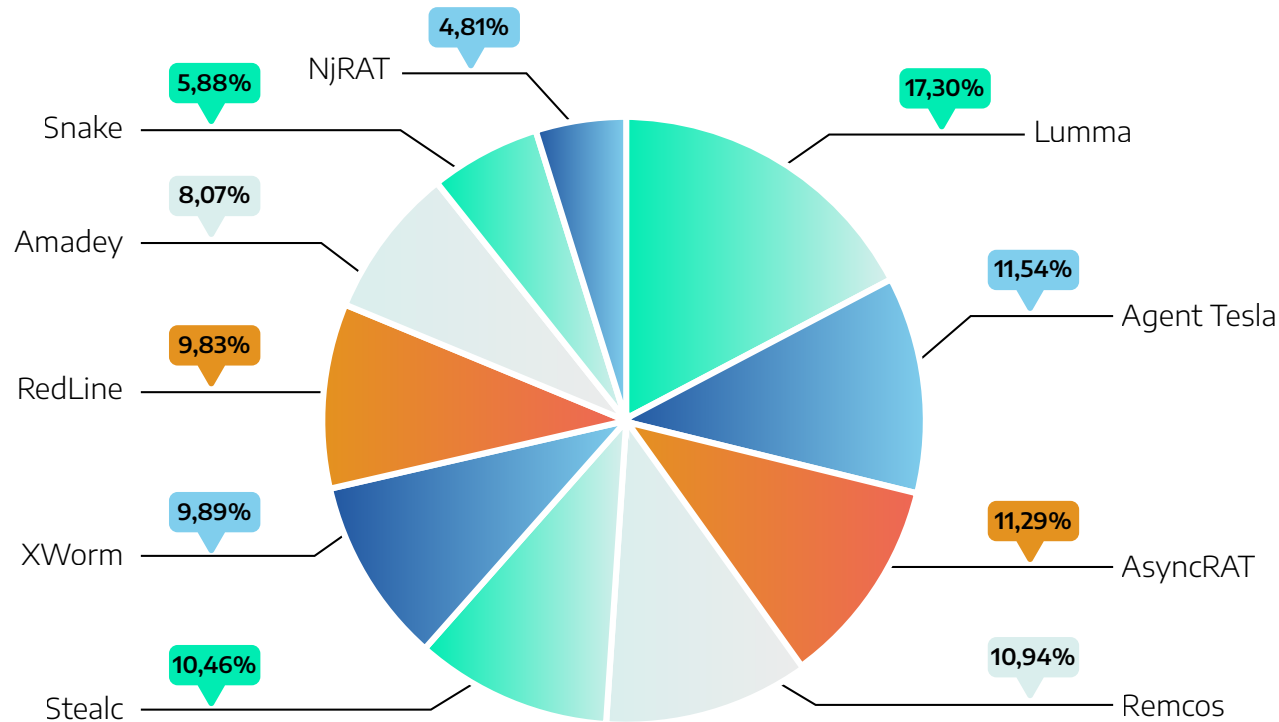
En 2024, trois familles de malware se distinguent.



**Lumma Stealer** apparaît comme l'un des *malwares as a service (MaaS)* les plus prolifiques cette année. A partir du second semestre, la popularité de cet infostealer se fait sentir alors qu'il passe devant les très populaires Remcos, AsynRat et AgentTesla.

Ces infostealers commercialisés alimentent le marché des Initial Access Brokers, vital pour les groupes de ransomware. Dans cet environnement compétitif, l'investissement dans l'amélioration de leurs capacités offensives a entraîné des remaniements constants dans le classement. La perturbation des réseaux cybercriminels menés par les autorités en 2024 contribue aussi à ce jeu d'échec.

### TOP DE FAMILLES DE MALWARE 2024



#### TOP 1



### LummaStealer

MaaS avec des fonctionnalités avancées vendu sous forme d'abonnements (jusqu'à 1000\$/mois). Au-delà des capacités d'exfiltration de données, il propose de multiples options d'évasion défensive rendant la détection complexe.

#### TOP 2



### AgentTesla

RAT très utilisé avec des capacités d'infostealer et de keylogger. Ce *malware as a service* est souvent utilisé par les courtiers d'accès initial dans les campagnes de phishing ciblé.

#### TOP 3



### AsyncRAT

RAT très populaire au sein de la communauté cybercriminelle du fait de son accès en open source. Disponible sur GitHub, il présente des fonctionnalités de keylogger, d'exfiltration d'accès initiaux, de dépôt de charge utile.



## LE BUSINESS LUCRATIF DES INFOSTEALERS

Ces dernières années, les actions défensives des Etats se sont multipliées. Coopération entre des entités publiques (polices nationales, Europol, FBI, etc.) et entités privées (entreprises de sécurité reconnues), ces opérations tendent à affaiblir les réseaux criminels. Elles démontrent des capacités offensives de la communauté internationale face à la recrudescence des cyberattaques sous toutes leurs formes.

### Course contre la montre

## OPERATION MAGNUS

Après l'opération Cronos qui a fortement impacté les activités de **LockBit**, voici venue l'**Opération Magnus**. L'action de coopération internationale du 28 octobre 2024 avait pour objectif de démanteler les réseaux d'infostealers **Redline et META**. Le succès de cette opération peut expliquer la disparition de MetaStealer du classement à partir de Q4 2024. Redline, un des MaaS les plus populaires, représentait près de **30%** du total des détections en 2023, Conséquence directe ou indirecte de l'opération, il perd sa place de leader et **descend au 7ème rang malgré un regain d'activité** sur la fin de l'année.

Ces opérations ont pour objectif de **perturber ces réseaux d'approvisionnement** et ont pour conséquence, même temporaire, de **réduire au global** les activités cybercriminelles qui fournissent des accès initiaux.

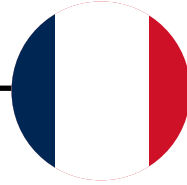


03.

## FUITES DE DONNÉES : UNE ANNÉE PRODUCTIVE POUR LES ATTAQUANTS

*Le nombre de fuites de données européennes est en partie biaisé en raison du manque de couvertures des fuites concernant les entités localisées dans certaines régions qui ne disposent pas de réglementations élaborées. Elles sont donc moins susceptibles de signaler des fuites de données.*

### LES FUITES DE DONNÉES EN FRANCE ET EN EUROPE



FRANCE

539

Les entreprises françaises ont été particulièrement touchées cette année par des fuites de données. Ce sont des milliers, parfois des millions de clients, dont les données sont exposées en ligne.

Cette inflation du nombre de données subtilisées peut avoir plusieurs explications :

- La France a particulièrement été mise en lumière sur la scène internationale cette année.
- Des attaquants qui seraient spécialisés dans la revente d'accès ou de base de données françaises.
- Des prestataires ont été compromis dans le cadre d'attaque de la chaîne d'approvisionnement.



EUROPE

2845

fuites de données  
depuis décembre 2023

Les investissements en matière de sécurité demeurent insuffisants, on observe de fortes inégalités au sein de l'Europe en raison des niveaux de maturité très variables d'un pays à l'autre.

Les pays du nord de l'Europe apparaissent plus sensibilisés notamment en raison de leur proximité avec la Russie, ce qui peut expliquer le nombre réduit d'incidents signalés si on les compare avec l'Europe de l'Ouest. Toutefois, la récente adhésion de la Suède et de la Finlande à l'OTAN met la résilience de leurs organisations et de leurs infrastructures à l'épreuve.

Parallèlement, une meilleure familiarisation avec les réglementations combinée aux exigences de mise en conformité encourage les organisations à signaler davantage les fuites de données. Ce chiffre pourrait encore augmenter avec la mise en place de DORA dès janvier 2025 qui exige des institutions financières qu'elles garantissent la sécurité de la transmission des données.



IMPACT

## FUITES DE DONNÉES : UNE ANNÉE PRODUCTIVE POUR LES ATTAQUANTS

Les organisations ciblées ont une vulnérabilité accrue au phishing et à l'ingénierie sociale. Les incidents de cette nature causent des dommages à l'image de l'entreprise et la confiance des clients, ce qui peut conduire indirectement à des pertes financières.

### La protection des données, un enjeu de lutte contre la cybercriminalité



#### Fuite de données record : France Travail et Cap Emploi dans le viseur des cybercriminels

Parmi les nombreuses attaques subies par la France, les bases de données de **France Travail et Cap Emploi contenant les données personnelles de 43 millions de personnes** (numéros de sécurité sociale, identité, adresse) ont été compromises. Cette violation massive de données ne manque pas de susciter l'intérêt des attaquants sur des forums cybercriminels compte tenu de l'ampleur des campagnes de phishing qui peuvent être menées.



#### Le Parlement européen, gardien du RGPD, à son tour exposé !

En dépit de son travail sur la protection des données, le Parlement européen n'est pas exempt des tentatives d'attaques. En mai 2024, une fuite de données qui a touché les ressources humaines du Parlement européen a été rendue publique. Elle a concerné **les données de 8 000 candidats à des contrats à durée déterminée** (cartes d'identité et passeports, extraits de casier judiciaire, documents de résidence, et même des informations sensibles comme les certificats de mariage qui révèlent l'orientation sexuelle d'une personne).

04.



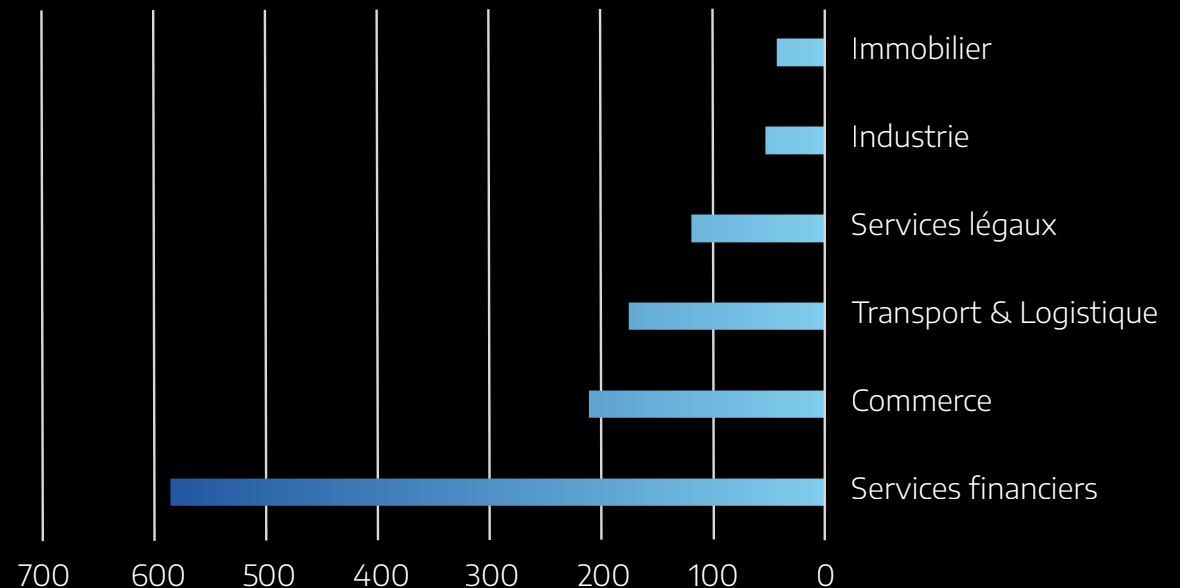
## L'OBSERVATOIRE CWATCH

Au travers de ses services, Almond accompagne ses clients à l'anticipation des menaces et participe à la protection du système d'information. Au quotidien, le SOC CWATCH surveille et détecte des incidents de sécurité de toutes natures.

### TOP 5 VICTIMOLOGIE CWATCH EN 2024

En 2024, le secteur des **services financiers** a été le plus touché par des tentatives de compromission et/ou des compromissions avérées, suivi par les secteurs du **commerce** et du **transport & logistique**.

Si les campagnes de phishing sont monnaie courante, les entités des secteurs **assurance** et **fonds d'investissement** en sont les premières victimes. Ces deux secteurs sont aussi particulièrement sensibles à la menace interne et notamment dans le contexte d'exfiltrations de données.



La surveillance des bases de données volées assure d'identifier rapidement les possibles points d'entrée via des **comptes valides**. Observables sur tous les périmètres, les secteurs **finance** et **commerce** sont particulièrement sujets à la compromission des comptes de leurs collaborateurs qui se retrouvent ensuite à la vente.



04.



## L'OBSERVATOIRE CWATCH

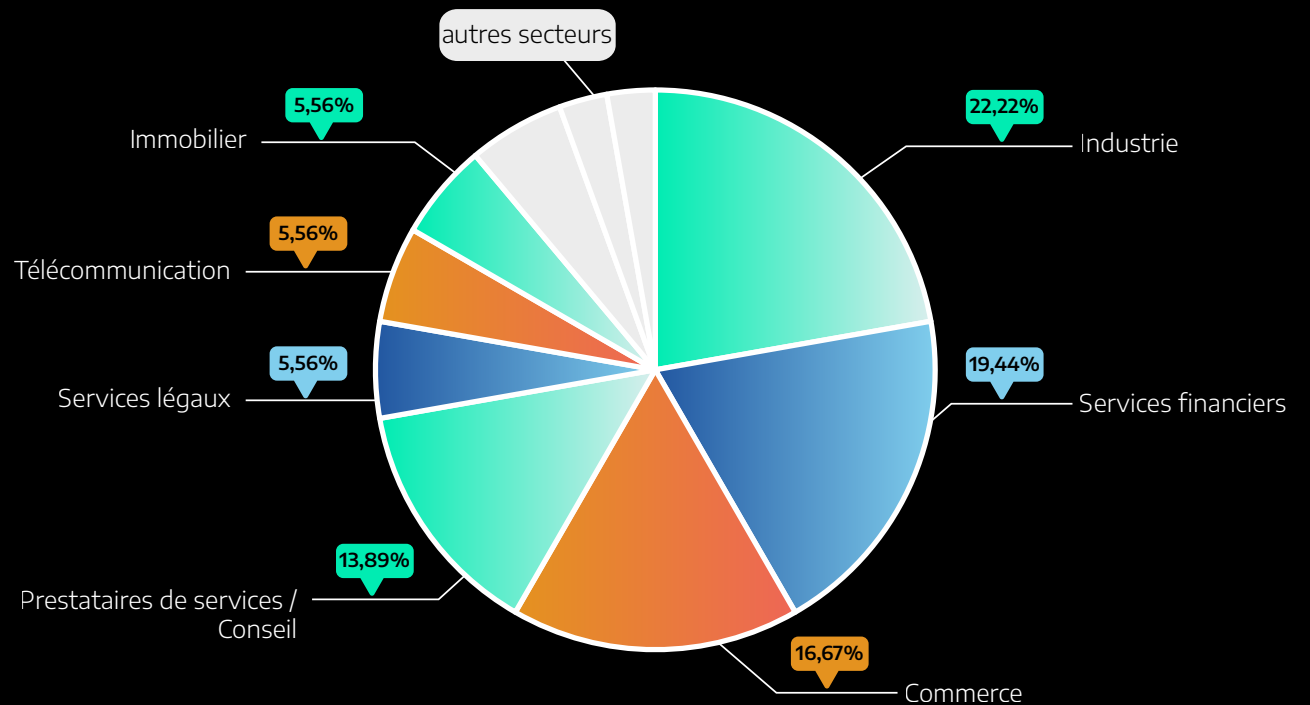
Le CERT CWATCH Almond a participé aux côtés de près de 80 CERT français à la première édition du [rapport d'incidentologie de l'InterCERT France](#).

**Almond a contribué à hauteur de 10% des incidents rapportés en 2023 dans le cadre de réponses aux incidents.**

### VICTIMOLOGIE DES RÉPONSES AUX INCIDENTS DU CERT

À l'échelle de CERT Almond, les secteurs de l'**industrie**, des **services financiers** et du **commerce** ont constitué une majeure partie des réponses aux incidents sur l'année.

La **santé**, le **conseil** et le **secteur des transports** arrivaient alors en tête du classement.





# L'OBSERVATOIRE CWATCH

Voir [l'infographie](#) sur les Jeux Olympiques

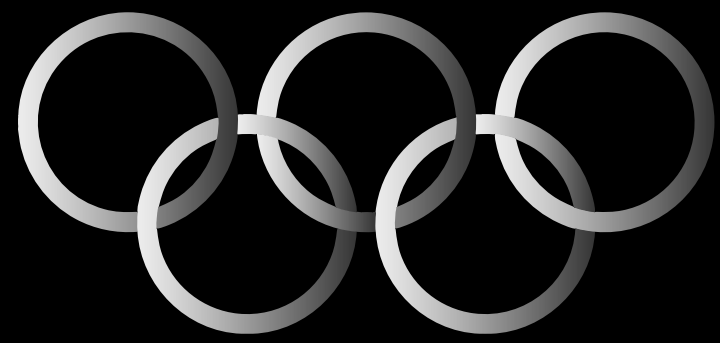


## Un été parisien sous le feu... Des médailles !

Pendant quatre ans, la France et les équipes de sécurité se sont préparées à une forte augmentation de l'activité cybercriminelle durant les Jeux Olympiques 2024 de Paris. Il semblerait que finalement les cybercriminels aient profité de leur été, car il n'y a pas eu d'incidents majeurs sur la période.

Avoir les projecteurs tournés vers la France pendant 4 semaines avec un **dispositif de sécurité rodé**, les **CERTs et SOC de France sur le qui-vive** et des **entreprises sensibilisées** pourraient avoir eu pour effet de dissuader les tentatives de compromission.

Encore une fois l'Armageddon n'aura pas eu lieu !



04.



## L'OBSERVATOIRE CWATCH

TTPs, Un faisceau d'offensives

**MITRE | ATT&CK®**

### TOP 10 DES TECHNIQUES MITRE ATT&CK 2024

**01**

[T1566]

**Phishing**  
Initial Access

**02**

[T1562]

**Impair Defenses**  
Defense Evasion

**03**

[T1078]

**Valid Accounts**  
Defense Evasion, Initial Access,  
Persistence, Privilege Escalation

**04**

[T1059]

**Command and  
Scripting Interpreter**  
Execution

**05**

[T1204]

**User Execution**  
Execution

**06**

[T1053]

**Scheduled Task/Job**  
Execution, Persistence,  
Privilege Escalation

**07**

[T1548]

**Abuse Elevation Control Mechanism**  
Defense Evasion,  
Privilege Escalation

**08**

[T1546]

**Event Triggered Execution**  
Persistence,  
Privilege Escalation

**09**

[T1584]

**Compromise Infrastructure**  
Resource Development

**10**

[T1651]

**Cloud Administration Command**  
Execution

05.

## DDOS : L'EUROPE DANS LE COLLIMATEUR



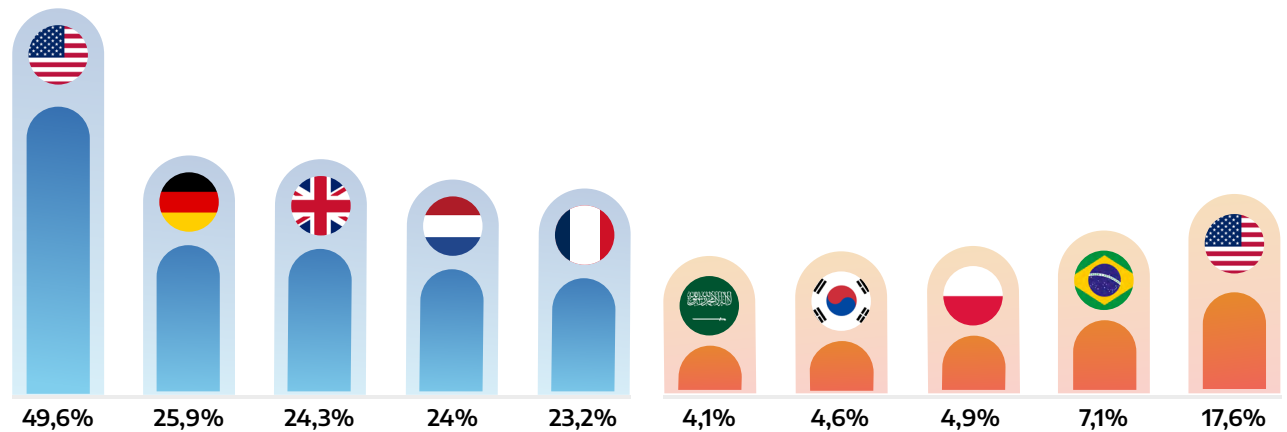
Déjà observée en 2023, la part des opérations de DDoS n'a cessé de croître en 2024.

L'intensification de la guerre en Ukraine, la recomposition des rapports de force au Proche et au Moyen-Orient en lien avec la chute du dirigeant syrien, le revers infligé à Moscou, l'accroissement des tensions au Pakistan, sont autant de revendications pour les groupes d'hacktivistes.

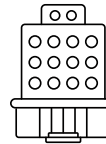
En dépit de l'intensité de ces événements, la majorité des attaques DDoS ont émané des **États-Unis**, de la **Grande-Bretagne** ainsi que de quelques **pays d'Europe de l'Ouest dont la France**.

### PAYS D'ORIGINE DES ATTAQUES DDOS

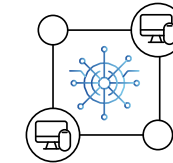
### PAYS DE DESTINATION DES ATTAQUES DDOS



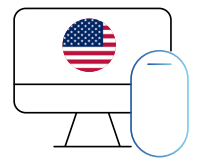
Les attaques de ce type, qu'elles soient perpétrées par un individu ou un groupe, utilisent un réseau compromis situé hors des frontières de la cible.



Le groupe Flax Typhoon utilise l'entreprise chinoise de cybersécurité Integrity Technology Group pour contrôler un botnet



Flax Typhoon contrôle **200 000** machines



Dont **100 000** machines aux États-Unis

### Exemple de Flax Typhoon, botnet chinois

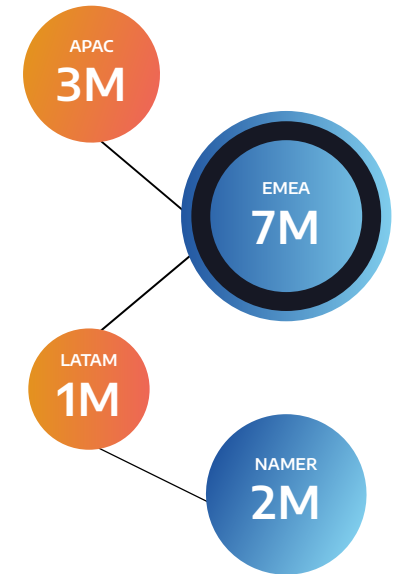
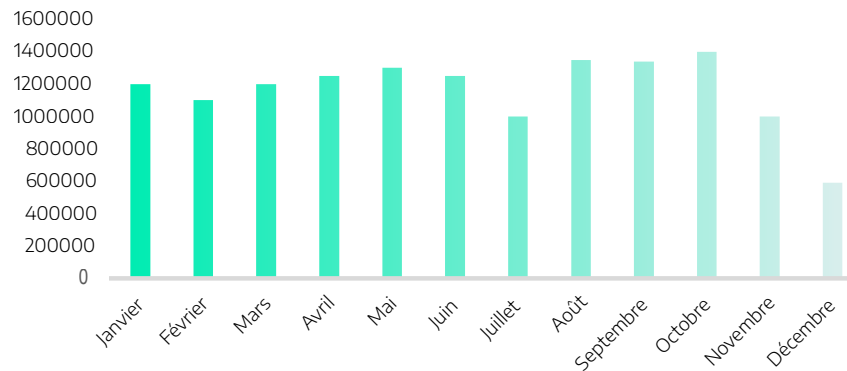
05

## DDOS : L'EUROPE DANS LE COLLIMATEUR

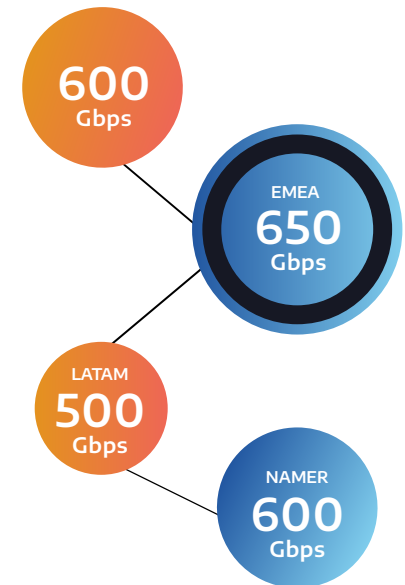
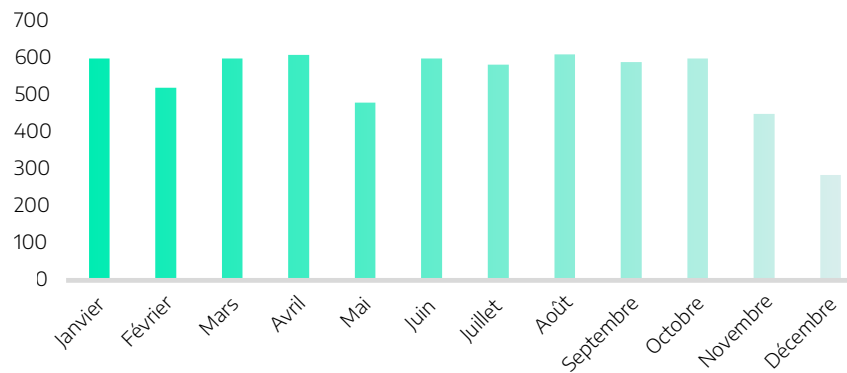


Au niveau mondial, la fréquence et le volume des attaques sont restés élevés et relativement stables. Une légère augmentation de la fréquence est observable de juillet à octobre.

### FRÉQUENCE DES ATTAQUES EN MILLIONS DANS LE MONDE



### VOLUME DES ATTAQUES EN GBPS DANS LE MONDE



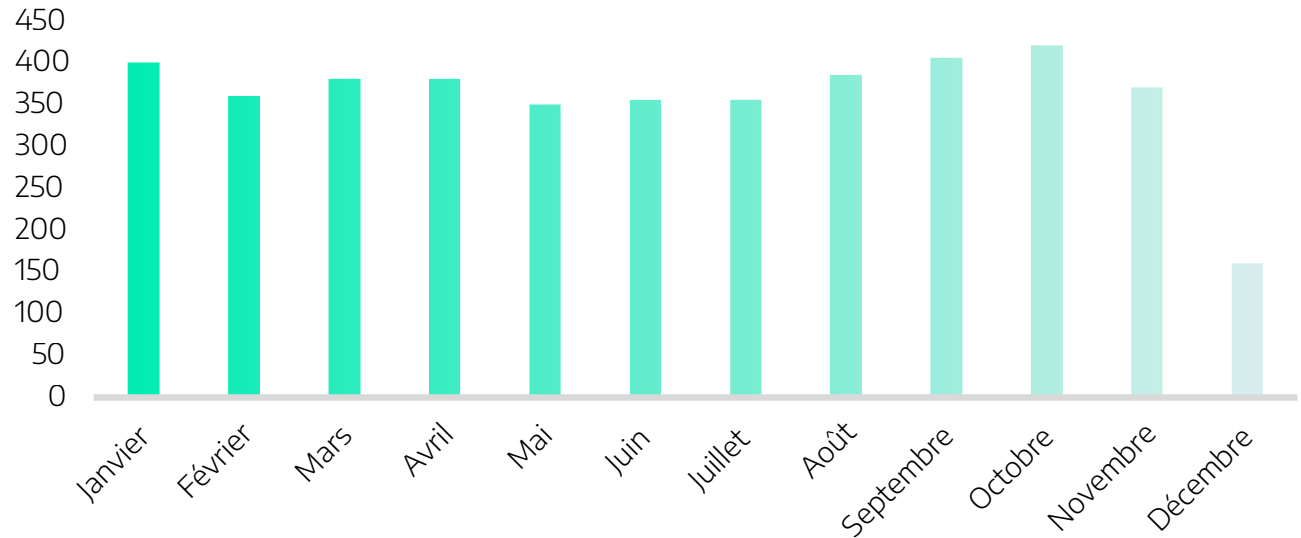
05.

## DDOS : L'EUROPE DANS LE COLLIMATEUR

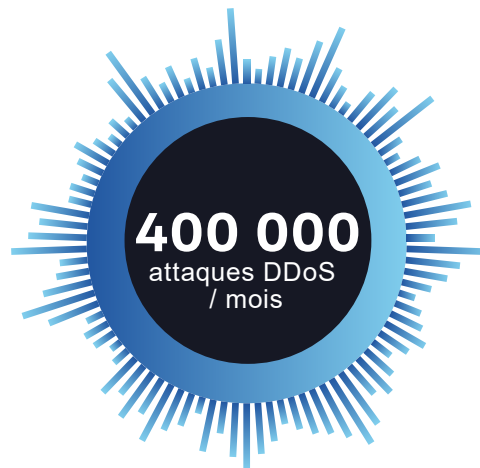


Les attaques de type DDoS sont de faible intensité, mais perturbent le cours des activités d'une organisation. Selon une étude conjointe menée par Splunk et Oxford Economics, la dégradation des services et les pannes coûtent 400 milliards de dollars par an aux entreprises du Global 2000.

### VITESSE DES ATTAQUES EN MPPS EN EUROPE



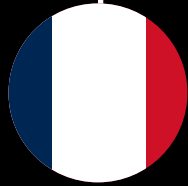
### MOYENNE DU VOLUME DES ATTAQUES EN EUROPE



Conséquence du positionnement des puissances européennes sur les **événements géopolitiques mondiaux**, les états européens ont subi de plein fouet toute l'année un niveau d'attaque élevé. Les attaques perpétrées dans le cadre du conflit entre la Russie et l'Ukraine sont susceptibles d'influencer les valeurs indiquées.

05.

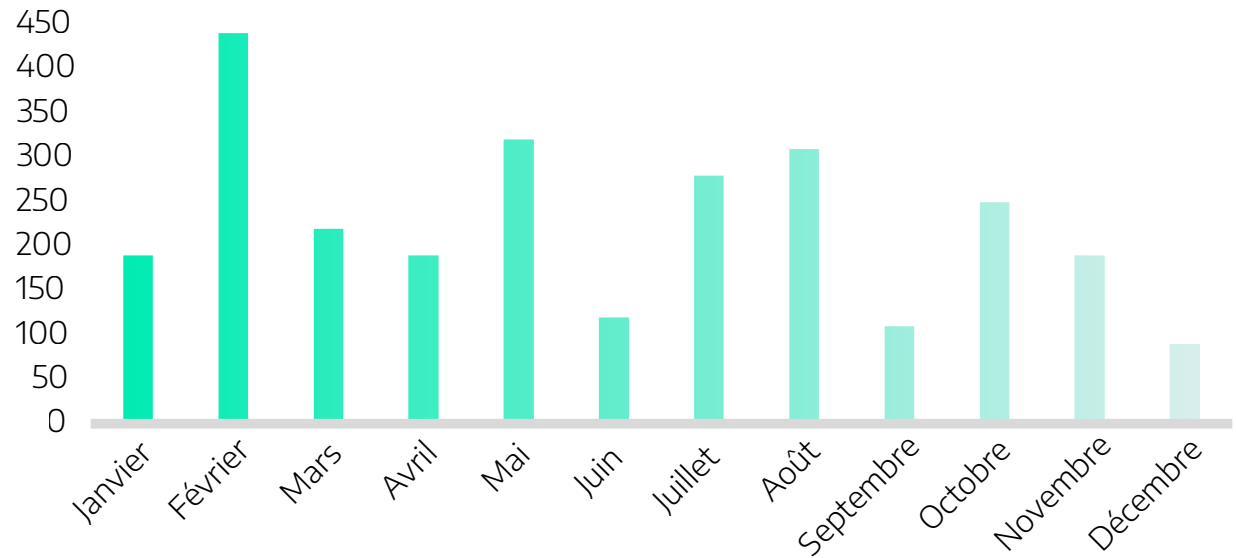
## DDOS : L'EUROPE DANS LE COLLIMATEUR



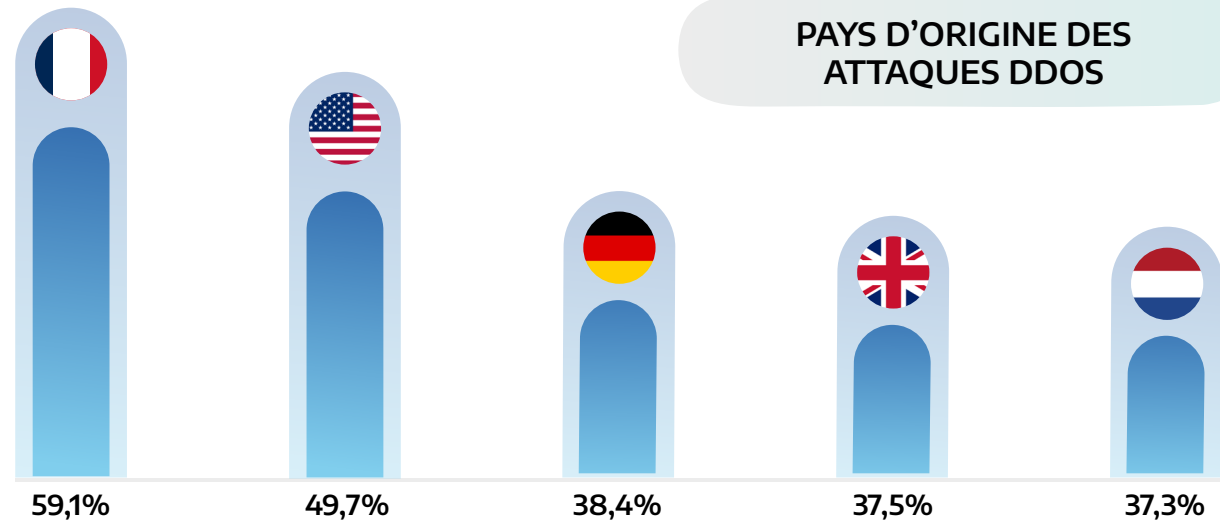
Les attaques subies en France proviennent principalement **des pays d'Europe de l'Ouest et des États-Unis**. La France étant en tête, il est possible que les attaquants français privilégient la compromission de machines situées sur leur territoire en raison de la proximité linguistique et culturelle.

Les attaques les plus rapides ont été menées en juillet 2024, correspondant au début des Jeux Olympiques de Paris. La sensibilité des entités ciblées peut expliquer la rapidité d'exécution des attaques.

### VOLUME DES ATTAQUES EN GBPS EN FRANCE



### PAYS D'ORIGINE DES ATTAQUES DDOS



Volume et pays d'origine d'attaques recensées ciblant la France





## DDOS : L'EUROPE DANS LE COLLIMATEUR

Les prises de position françaises sur l'Ukraine et Israël ont renforcé son exposition aux cyberattaques en 2024, en particulier des campagnes de DDoS. La coalition d'hacktivistes « **Holy league** » est apparue en juillet. Constituée de près de 70 membres, elle s'unie **contre l'Europe, l'Ukraine, Israël et l'OTAN**. Profitant du flottement politique du gouvernement, plusieurs groupes tels que **NoName057(16)**, **Mr. Hamza**, **Anonymous Guys** ont attaqué des entités privées et publiques françaises en fin d'année.

Le groupe **NoName057(16)** qui a d'ailleurs joué un rôle central dans cette recrudescence d'attaques DDoS contre la France au-delà de la coalition tout comme **RipperSec**.

## Représailles géopolitiques

### Février 2024

Déclaration du Président de la République au sujet du déploiement des forces armées européennes en Ukraine.

### Mars 2024

- Russie : Attentat à Moscou, qui aurait pu être organisé par l'Etat français selon le Kremlin.
- France : Attaques d'ampleur inédite revendiquées entre autres par **Anonymous Sudan**. Le caractère critique des entités visées peut expliquer une légère hausse de la vitesse en mars.

### Août 2024

Tenue des Jeux Olympiques à Paris et de Pavel Duro. en raison de ses actions limitées menées pour juguler la prolifération des activités cybercriminelles sur la plateforme.

### Décembre 2024

Plusieurs groupes d'hacktivistes ont profité de la démission de Michel Barnier pour cibler une cinquantaine de sites français, principalement des sites de l'Etat.

Pinned message  
ANNOUNCEMENT Greetings Ladies & C

**EVERT KIPPERSEC ATTACK**

ANNOUNCEMENT

- 1. THAILAND :**
  - We attack Thailand because Thailand killing Innocent Muslims (Malay) in Pattani. They also stole Malay land (Patani, Yala, Naratiwat).
- 2. ISRAEL :**
  - We attack Israel because Israel killing Innocent Muslims in Palestine and Lebanon.
- 3. TAIWAN :**
  - We attack Taiwan because Taiwan makes bomb to help Israel killing Lebanon People. They supporting Israel & They trying to insult Russia.
- 4. AMERICA (USA) :**
  - We attack America because Biden supplying Money & Weapon to killing Innocent people in Palestine & Lebanon.
- 5. UNITED KINGDOM :**
  - We attack United Kingdom because they supplying Money and Support Israel to kill Innocent people in Palestine & Lebanon.
- 6. FRANCE :**
  - We attack France because they Supply Weapon to Israel to killing Innocent people in Palestine & Lebanon.
- 7. INDIA :**
  - We attack India because they killing Muslims in their Country, They insulting Muslims and the Supporting Israel.



## DDOS : L'EUROPE DANS LE COLLIMATEUR

Les attaques les plus rapides ont été menées en juillet 2024, ce qui correspond au début des Jeux Olympiques. La sensibilité des entités ciblées peut expliquer la rapidité d'exécution des attaques.

### Attaques hyper-volumétriques

L'adoption de l'IA pour assister les cybercriminels dans la conduite de leurs attaques utilisant des botnets permet d'en améliorer l'efficacité notamment en facilitant le contournement des mesures défensives et en imitant le trafic légitime.

Elles utilisent d'énormes volumes de trafic pour surcharger le réseau d'une cible

Elles génèrent d'énormes volumes de bande passante (jusqu'à 100 Gbps, voire des téraoctets par seconde)

Elles utilisent de gigantesques réseaux de machines compromises composés de dizaines ou de centaines de milliers d'appareils

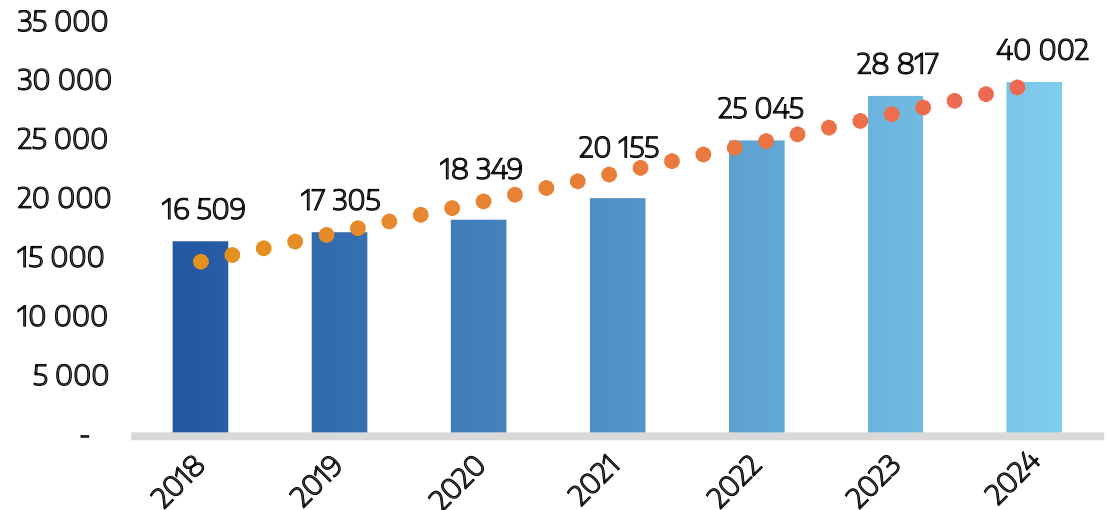
Il est donc presque impossible pour les cibles de se défendre contre ces attaques. Les attaques hyper-volumétriques sont un sous-ensemble d'un modèle plus large d'attaques DDoS qui deviennent de plus en plus complexes et puissantes. Pour dissimuler des attaques plus ciblées, elles mélangent souvent des attaques volumétriques et des attaques au niveau de la couche applicative.

06

## VULNÉRABILITÉS : LE POIDS SUR LES STRATÉGIES DÉFENSIVES

L'année 2024 a encore été marquée par un accroissement des vulnérabilités. L'impact visible est l'incapacité pour les entités de prendre en compte ce volume dans leurs programmes de patch management (si existants), car cela représente un coût considérable. Face à cette course effrénée, peut-on trouver une explication à ce phénomène qui ne semble pas vouloir ralentir.

### VULNÉRABILITÉS EN 2024



### LES CLÉS DE COMPRÉHENSION

De nouveaux produits entrent sur le marché chaque année avec leur lot de vulnérabilités. Rapportées au nombre de solutions existantes, peut-on affirmer que le nombre de vulnérabilités suit la même courbe ?

Aujourd'hui les données se basent sur les CVE répertoriées par le NVD sur l'année. Les vulnérabilités sans CVE ou les vulnérabilités des produits en SaaS ne sont pas prises en compte et pourraient aussi influencer sur le volume total.

De plus en plus d'entreprises spécialisées ont pour business model la découverte et publication de vulnérabilité, ce qui pourraient expliquer en partie la hausse de la volumétrie chaque année.

Dans le lot des vulnérabilités publiées sont parfois intégrés les bugs et les erreurs de configuration qui au sens de sécurité n'en sont pas réellement.

06

## VULNÉRABILITÉS : LE POIDS SUR LES STRATÉGIES DÉFENSIVES

*Un autre système de scoring EPSS a été introduit en plus du score CVSS pour aider les organisations à mieux prioriser la gestion des vulnérabilités, basé non sur la criticité, mais sur l'exploitation réelle. Néanmoins, certaines vulnérabilités, pourtant identifiées comme exploitées par des APT ou des groupes de ransomware, ont des scores CVSS et/ou EPSS faibles. Si les scores permettent le tri dans le volume de données, il reste indispensable que le sujet de la gestion des vulnérabilités soit abordé de manière transverse entre des équipes de Cyber Threat Intelligence, le RSSI et les équipes de patch afin de prendre des décisions contextualisées et éclairées.*

### RÉTROSPECTIVE SUR LES VULNÉRABILITÉS 2024

Sur l'année 2024, 2 291 vulnérabilités critiques ont été répertoriées par le NVD, soit évolution de 44% par rapport à 2023. Si on se penche sur les CVE exploitées, sans critère de sévérité, le [catalogue KEV](#) en décompte 186. Celles-ci représentent 0.5% du total de vulnérabilités remontées sur l'année. Dans le [Threat Landscape 2023](#), nous observions déjà un début d'année 2024 marqué par le ciblage d'outils largement utilisés par les entreprises dans le monde. Force est de constater que la tendance s'est confirmée avec le trio Ivanti, Fortinet et PaloAlto. Les équipements de ces éditeurs ont été parmi les plus visés en termes d'exploitation de vulnérabilités critiques.

#### Fortinet

##### Février 2024

CVE-2024-21762, an out-of-bound write flaw in Fortinet FortiOS; score CVSS 9.8 et score EPSS 2.11%

##### Octobre 2024

CVE-2024-47575, a Missing authentication in FortiManager; score CVSS 9.8 et score EPSS 88.63%

#### PaloAlto

##### Avril 2024

CVE-2024-3400, a command injection flaw in Palo Alto Networks PAN-OS score CVSS 10; score EPSS 96.37%

##### Novembre 2024

CVE-2024-9474, a privilege escalation vulnerability in Palo Alto Networks PAN-OS software; score CVSS 7.2; score EPSS 97.52%

#### Citrix

##### Janvier 2024

CVE-2023-6549, an improper Restriction of Operations within the Bounds of a Memory Buffer in NetScaler ADC and NetScaler Gateways; score CVSS 7.5 et score EPSS 1.23%

#### Ivanti

##### Janvier 2024

CVE-2024-21887, a command injection flaw in Ivanti Connect and Policy Secure; score CVSS 9.1 et score EPSS 97.11%

CVE-2023-46805, a remote authentication bypass flaw in Ivanti Connect and Policy Secure; score CVSS 8.2 et score EPSS 96.41%,

CVE-2024-21893, an elevation of privilege flaw in Ivanti Connect and Policy Secure score CVSS 8.2 et score EPSS 95.90%

#### Cisco

##### Juillet 2024

CVE-2024-20399, a command line interface command injection flaw in Cisco NX-OS Software; CVSS 6.7; score EPSS 0.25%

#### Microsoft

##### Mars 2024

CVE-2024-26169, Windows Error Reporting Service Elevation of Privilege Vulnerability; score CVSS 7.8; score EPSS 0.67%



# RÉFÉRENCES

<https://www.lebigdata.fr/ce-celebre-club-de-foot-frappe-par-un-ransomware-les-donnees-des-supporters-en-fuite>

<https://www.lemagit.fr/actualites/366599633/Ransomware-75-millions-de-dollars-la-rancon-record-obtenue-par-Dark-Angels>

<https://therecord.media/ransomhub-cybercrime-coppell-texas-minneapolis-parks-agency>

<https://www.oxfordeconomics.com/resource/the-hidden-costs-of-downtime-the-400b-problem-facing-the-global-2000/>

<https://www.euronews.com/next/2024/08/22/european-parliament-under-scrutiny-after-data-breach-complaints>

[https://www.francetvinfo.fr/replay-radio/le-choix-franceinfo/piratage-de-france-travail-la-direction-avait-ete-alertee-sur-une-faille-de-securite\\_6536786.html](https://www.francetvinfo.fr/replay-radio/le-choix-franceinfo/piratage-de-france-travail-la-direction-avait-ete-alertee-sur-une-faille-de-securite_6536786.html)

<https://cyble.com/blog/hacktivist-alliances-target-france/>

<https://www.helpnetsecurity.com/2024/02/22/stolen-credentials-exploit/>

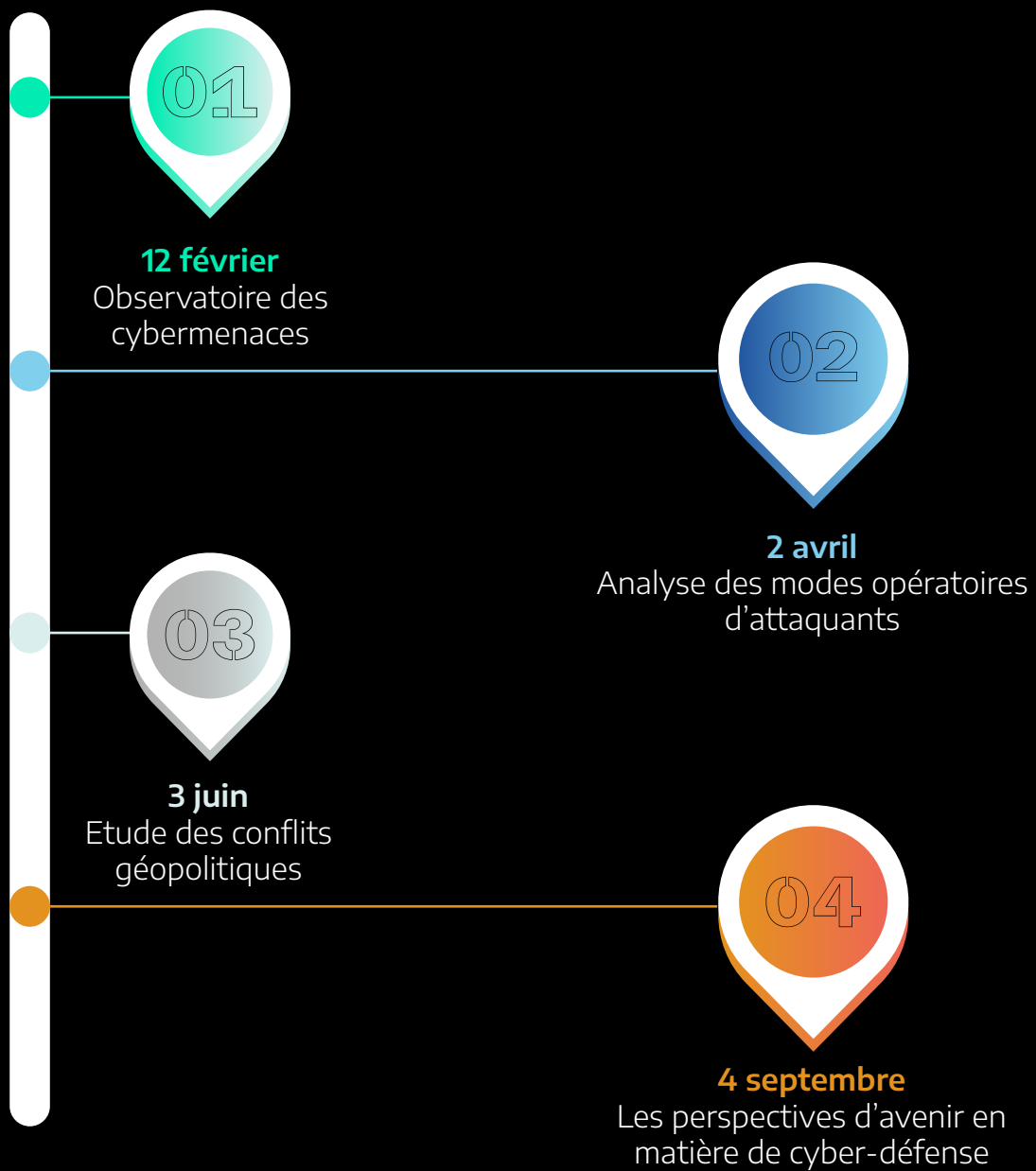
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

<https://any.run/cybersecurity-blog/>

<https://nvd.nist.gov/>

<https://tribune-assurance.optionfinance.fr/depeches/d/2024-10-17-qbe-une-hausse-de-74-des-attaques-par-ransomware-en-2023.html>

# CALENDRIER 2025





# Almond

→ [contact@almond.eu](mailto:contact@almond.eu)  
→ 01 46 48 26 00